スマートフォンのセキュリティ

KDDI研究所
竹森 敬祐

PCと何が違うの？
脅威と注意点を整理しよう！

1: スマートフォンの概要
2: Android™フォンのセキュリティ
3: KDDIの取り組み
4: まとめ ～現状と今後の課題～

Android™は、Google Inc. の商標または登録商標です。

スマートフォンの定義

- 汎用OS
  - PCに、電話アプリが搭載された携帯端末（携帯情報処理設備）
- ディスク領域
  - 端末メーカや通信キャリアが管理するシステム領域と、アプリ開発者や利用者に解放されたユーザ領域が分かれた携帯端末
- サービス
  - 電気通信事業法に従う通信キャリアのサービスと、世界の潮流をいち早く取り込むインターネット業界のサービスが混在する携帯端末
  - 安全性重視の通信キャリアのサービスと、利便性重視のインターネット業界のサービスが混在する携帯端末
- 世界標準
  - 世界基準の安全性（＝自己責任）が持ち込まれた携帯端末

スマートフォンの特徴

■ スマートフォンの定義 （利便性）

(1) 誰もがアプリケーション（以下、アプリ）の開発を行える。
(2) 誰もがアプリのインストールを行える。
(3) PC向けの汎用OSをベースとした様々な処理機能を持つ。

■ セキュリティ対策 （安全性）

(1) アプリを安全に実行する制御の壁（サンドボックス）を設けている。
(2) 悪意のソフトウェア（マルウェア）への感染を防ぐアプリ配信（Marketプレイス）の安全化が図られている。
(3) PCと同様なセキュリティパッチの適用が行われている。

★ 通常利用で脅威は少ないが、悪性アプリ（マルウェア）への手動感染と、利用者自身による端末への攻撃（管理者権限奪取）で、PCと同様＋αの脅威がある。

■ 展開モデル

◆ 垂直統合型：端末／OS／アプリ／通信をクローズドに管理
◆ 水平展開型： “ をオープン化して役割分担

注）事項以降、数あるスマートフォン向けOSのうち、仕様が公開されているAndroid™フォンが議論しやすいため、こちらを例に詳解します。

スマートフォンのセキュリティ

KDDI研究所
竹森 敬祐

1: スマートフォンの概要
2: Android™フォンのセキュリティ
3: KDDIの取り組み
4: まとめ ～現状と今後の課題～

Android™は、Google Inc. の商標または登録商標です。

はじめに　～セキュリティ面での比較～

	従来の携帯	Android™フォン	PC
OS/開発情報 （脆弱性）	クローズ （限定的）	オープン （多数が公知化）	汎用OS （多数が公知化）
API （サンドボックス）	限定的 （全アプリへ強制）	豊富＋ユーザ承認 （全アプリへ承認型）	豊富 （Webブラウザのみ）
端末識別子管理	強（堅牢に保護）	弱（APIアクセス可）	ー
コンソール	無	有	有
ディスクの暗号化	無	限定的	有
遠隔ロック・ワイプ	有	有	無
アプリ販売（Market）	クローズ	オープン	オープン
管理者権限アプリ	無	無　＊	有
マルウェア感染	限定的	有（手動）	有（手動 & 自動）
Webスクリプト攻撃	限定的	有	有
フィッシング	有	有	有
総合的な安全度	★★★	★★	★

＊ 想定外の管理者権限奪取や管理者権限利用のアプリがある。

最大の脅威

Android™のセキュリティ機構 ～Android Market™～

■ マルウェア感染の導線
- ◆ ユーザが直面する脅威の殆どは、Marketプレイスからアプリをインストールする行為で生じる。
  - ◆ 一部は、PCからUSB経由（adbシェル）のアプリのインストールで生じる。
  - ◆ 一部は、メール添付アプリのインストールで生じる。
- ★ マルウェアをクリックするだけで感染しない！

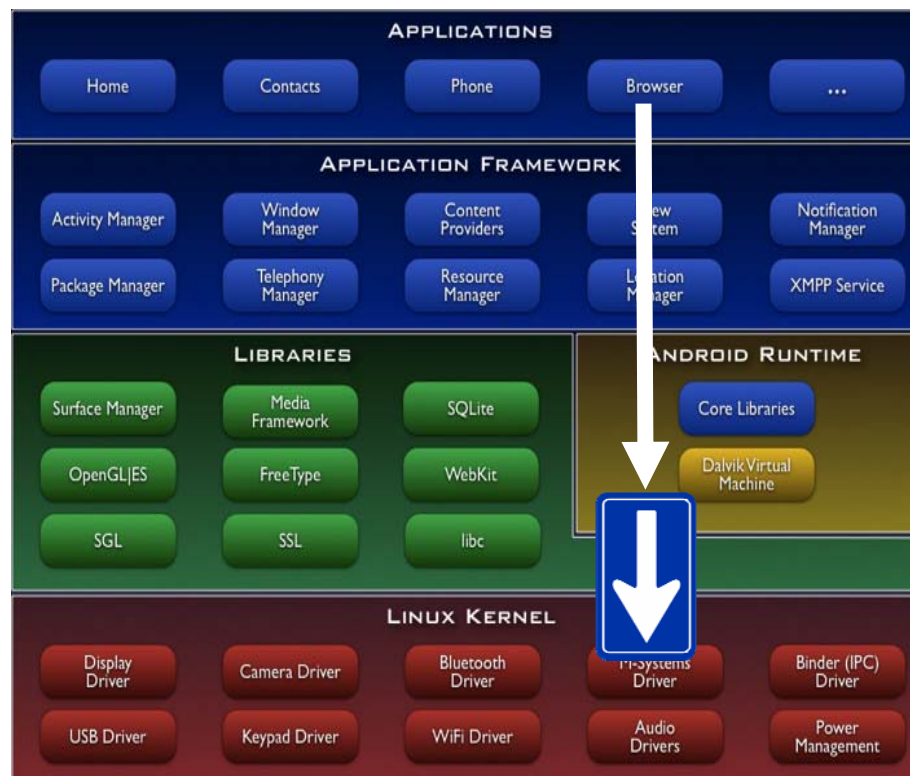
■ Googleの取り組み
- ◆ Android Market™では開発者登録としてクレジットカードを登録し$25を支払う。
  ⇒ マルウェア掲載の頻度は少ない。
- ◆ ユーザからの指摘を受けて迅速にマルウェアを駆除する事後対応を行っている。
  ⇒ 感染者は少ない。

Android Market™

Android™のセキュリティ機構 ～サンドボックス～

■ Linux OS + サンドボックス

◆ Linuxカーネルの上に、パーミッション可変型のサンドボックスを構築したOS。
⇒ 安全性と利便性のトレードオフをユーザに委託する、可変型サンドボックス。

◆ アプリが利用する機能・情報をユーザが承認することで、実行権が決まる。
⇒ 手動承認のため、自動感染型ウイルス・ワームへの脅威は小さい*。

* 管理者権限が奪われた場合、
自動感染はありうる。

可変型（ユーザ承認型）
サンドボックス

Android™OSから求めるユーザ承認

■ パーミッション機構

◆ Android™OSから、アプリが利用する機能や情報を表示して、ユーザ承認を求めるインストール機構となっている（Android Market™はFunction表示でユーザ許諾を得る）。

⇒ 機能や情報を利用する目的が記されていない。

⇒ 機能や情報単位で申請であり、総合的な作用や悪意の判断は難しい 。

★ この機構でユーザ承認を得ているものの、アプリ側からの説明も望まれる。

パーミッションの利用実態 ～統計調査(2011年8月)～

- Android Market™の無料アプリ(14カテゴリ×70個＝980個)のパーミッション
  - 携帯電話特有の情報を利用するアプリが多数ある。その多くが広告機能を内包。
  - 2010⇒2011急増: 情報収集モジュールを組み込んだアプリが増えた？

参考:2010年	順位	合計 980	利用率	Android Permission	説明 (au one Marketでの説明文)
→ 55.4%	1	882	90.0%	INTERNET	インターネットへのアクセス
	2	664	67.8%	WRITE_EXTERNAL_STORAGE	SDカードへの情報の書き込み
	3	575	58.7%	ACCESS_NETWORK_STATE	ネットワークへの接続状態の表示
→ 17.2%	4	567	57.9%	READ_PHONE_STATE	電話番号やSIM情報の読み取り
	5	287	29.3%	VIBRATE	バイブレーション機能
→ 15.8%	6	278	28.4%	ACCESS_COARSE_LOCATION	携帯電話基地局情報やWiFiアクセスポイントを使った位置情報の取得(精度低)
→ 15.2%	7	261	26.6%	ACCESS_FINE_LOCATION	携帯電話基地局情報やWiFiアクセスポイント、及び、GPSを使った位置情報の取得(精度高)
	8	243	24.8%	WAKE_LOCK	端末のスリープの無効
	9	160	16.3%	ACCESS_WIFI_STATE	Wi-Fiアクセスポイント情報の表示
	10	122	12.4%	RECEIVE_BOOT_COMPLETED	端末起動時にアプリケーションを自動的起動

情報収集モジュールの実態

■ ターゲット広告

◆ アプリ内の広告をユーザがクリックすることで、開発者に報酬が入る。

⇒ READ_PHONE_STATE: Android ID、電話番号などからユーザを識別。

⇒ ACCESS_COARSE(FINE)_LOCATION : 場所に応じた広告を表示。

■ 望ましい姿

◆ Android™の安全機構（パーミッション）でユーザから承諾は得ているものの、情報収集モジュールを組み込んだアプリ開発者はユーザに対して収集する情報、利用目的や範囲などをアプリの中で説明／許諾を得た方が親切。

検索アプリ

■ 情報収集モジュールの含有実態

◆ Android Market™の14カテゴリ×70個＝980個の無料アプリを対象に含有する情報収集モジュールを調査。

	含有数	含有率
アプリ総計	558/980	56.9%
情報収集モジュール総計	1065/558	1.91個

マルウェア　～①パーミッション悪用型～

■ 偽のオンラインバンキング管理アプリ

◆ オンラインバンキングアプリにキロガーが内包されていた。

READ_INPUT_STATE

■ 偽のマルウェア対策アプリ

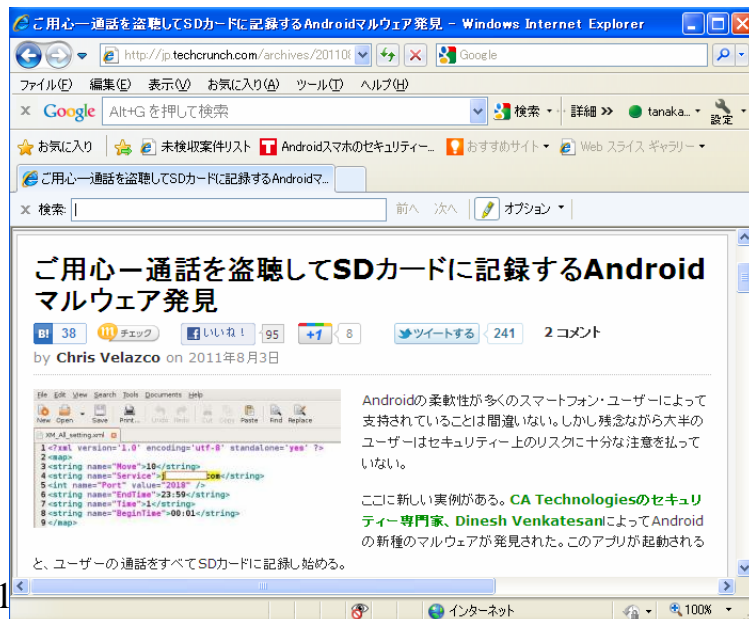
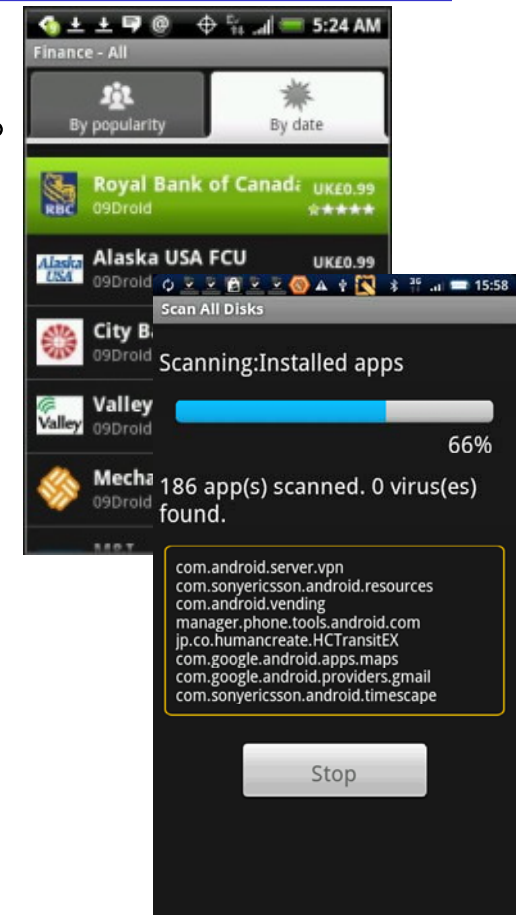
◆ 何も検知しないマルウェア対策ソフトが、情報を漏洩する。

INTERNET、DELETE_PACKAGES、RESTART_PACKAGES、READ_PHONE_STATE、RECEIVE_SMS、READ_CONTACTS、WRITE_CONTACTS、CALL_PHONE、READ_SMS、WRITE_SMS、SEND_SMS、GET_TASKS、RECEIVE_BOOT_COMPLETED、INSTALL_PACKAGES、ACCESS_NETWORK_STATE、WRITE_APN_SETTINGS、PROCESS_OUTGOING_CALLS、INSTALL_SHORTCUT、LOCATION、ACCESS_FINE_LOCATION、ACCESS_LOCATION_EXTRA_COMMANDS、ACCESS_MOCK_LOCATION、ACCESS_COARSE_LOCATION、ACCESS_COARSE_UPDATES、CALL_PRIVILEGED、MODIFY_PHONE_STATE、GOOGLE_AUTH.mail、WAKE_LOCK、WRITE_EXTERNAL_STORAGE、USE_CREDENTIALS、VIBRATE

ご用心ー通話を盗聴してSDカードに記録するAndroidマルウェア発見

by Chris Velazco on 2011年8月3日

Androidの柔軟性が多くのスマートフォン・ユーザーによって支持されていることは間違いない。しかし残念ながら大半のユーザーはセキュリティー上のリスクに十分な注意を払っていない。

ここに新しい実例がある。CA Technologiesのセキュリティー専門家、Dinesh VenkatesanによってAndroidの新種のマルウェアが発見された。このアプリが起動されると、ユーザーの通話をすべてSDカードに記録し始める。

■ 盗聴アプリ

◆ 通話音声をSDカードへ記録する。

◆ その後、ファイル交換アプリで漏洩する。

WRITE_EXTERNAL_STRAGE

http://jp.techcrunch.com/archives/20110802android-malware-eavesdrops-records-your-conversations/

マルウェア　～②脆弱性攻撃型～

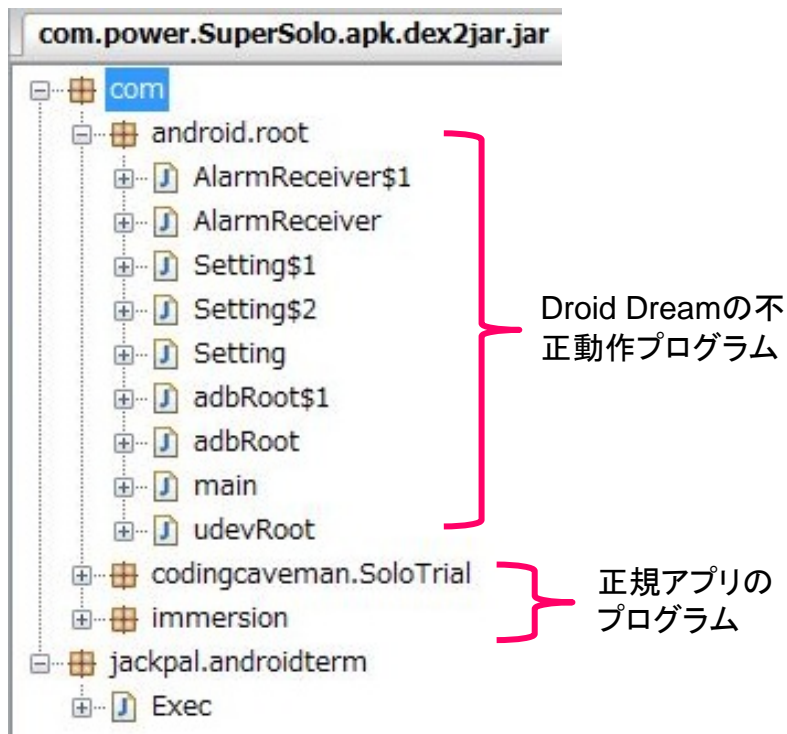
■ アップデート型のDroid Dream

◆ 正規アプリに攻撃コードを埋め込み、Android Market™で公開した。

◆ 管理者権限を奪い、別マルウェアを外部から取得し、/system/appへ保存する。

⇒ 脆弱な端末のユーザを騙すことで、管理者権限を密かに奪う。

⇒ 別のマルウェアを取得し、自動アップデート（サイレントインストール）する。

⇒ 一般権限で駆除できない。単純なアンインストールで駆除しきれない。

開発者	Myournet	Kingmall2010	we20090202
アプリ名	Falling Down	Bowling Time	Finger Race
	Super Guitar Solo	Advanced Barcode Scanner	Piano
	Super History Eraser	Supre Bluetooth Transfer	Bubble Shoot
	Photo Editor	Task Killer Pro	Advanced Sound Manager
	Super Ringtone Maker	Music Box	Magic Hypnotic Spiral
	Super Sex Positions	Sexy Girls: Japanese	Funny Face
	Hot Sexy Videos	Sexy Legs	Color Blindness Test
	Chess	Advanced File Manager	Tie a Tie
	下坠滚球_Falldown	Magic Strobe Light	Quick Notes
	Hilton Sex Sound	致命绝色美腿	Basketball Shot Now
	Screaming Sexy Japanese Girls	墨水坦克Panzer Panic	Quick Delete Contacts
	Falling Ball Dodge	裸奔先生Mr. Runner	Omok Five in a Row
	Scientific Calculator	软件强力卸载	Super Sexy Ringtones
	Dice Roller	Advanced App to SD	大家来找茬
	躲避弹球	Super Stopwatch & Timer	桌上曲棍球
	Advanced Currency Converter	Advanced Compass Leveler	投篮高手
	App Uninstaller	Best password safe	
	几何战机_PewPew	掷骰子	
	Funny Paint	多彩绘画	
	Spider Man		
	蜘蛛侠		

3名の攻撃者が50のアプリに埋め込んだ。

2つに分類されるAndroid™マルウェア

	マルウェア	
	①パーミッション悪用型	②脆弱性攻撃型
感染	ユーザによる手動インストール。 手動・自動起動で影響が出る。	ユーザによる手動インストール。 OSの脆弱性を突いて管理者権限を一時的・恒久的に奪う。
実体	悪性モジュール	攻撃コード + 管理者権限へ昇格(su)コマンド
権限	一般権限 過剰なAndroidパーミッション	管理者権限
被害	情報漏洩、踏み台(なりすまし、ボット)、不正課金	情報漏洩、踏み台(なりすまし、ボット)、管理者権限利用(改造)
他者連携	他のアプリが持つパーミッションと連携することで新たな脅威が生じる。	他のアプリに奪った管理者権限を提供する。
Market掲載	マルウェアと判定され難く、掲載され続けることが多い。	管理者権限を奪うアプリ:排除 管理者権限を利用するアプリ:掲載
駆除	アンインストールで完全に消去できる。	/system領域を改造された場合、アンインストールや工場出荷状態の初期化が困難。

ところで、マルウェアの出現状況

■ PC･モバイルの総計（2011年1月～2011年10月観測）
- ◆ のべ1,300,000種類、約4,300種類／日の検体を観測。

■ Androidの統計（2011年1月～6月観測）
- ◆ のべ200種類、約1.1種類／日の検体を観測。

マルウェア出現数　PC : Android™フォン ＝ 4000 : 1
（Android™フォンのマルウェア感染は殆ど無く、PCよりもかなり安全）

勝手な情報送信の主原因は、アプリ開発者による情報収集モジュールの誤用です。
ターゲティングサービスのため本件の実被害報告はない。

マルウェア対策ソフトの検知対象外

統計情報の提供元
株式会社カスペルスキー

スマートフォンのセキュリティ

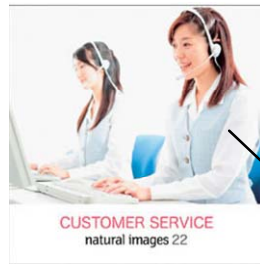
KDDI研究所
竹森 敬祐

KDDIの独自の取り組みをご紹介します！

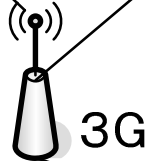
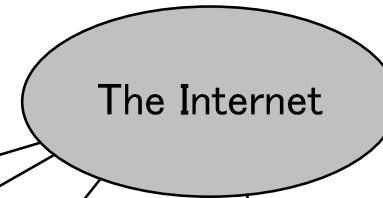
1: スマートフォンの概要
2: Android™フォンのセキュリティ
3: KDDIの取り組み
4: まとめ ～現状と今後の課題～

Android™は、Google Inc. の商標または登録商標です。

はじめに　～セキュリティマップ～

・お客様への説明
・情報発信

(4) ネットワークのセキュリティ
・ネットワークの安定化

The Internet

通信キャリア
NW

3G

WiFi

(2) Marketのセキュリティ
・公開アプリの事前審査
・安全な課金スキーム

・開発者への啓発
・著作権重視のアプリ

(1) 端末のセキュリティ
・セキュリティパッチ
・リモートロック／ワイプ
・マルウェア対策ソフト

(0) 脆弱性の調査
・原因調査
・実証実験

「脆弱性の調査」と「端末のセキュリティ」

■ 脆弱性の調査・対策指導

◆ 普及期は、グローバル端末をそのまま日本市場に投入するのは不親切と考えている。

⇒ セキュリティインシデントの調査・分析を進めてきた（右表）。

⇒ 端末ベンダ等へ、脆弱情報をフィードバックすることで迅速にパッチをリリース。

インシデントの収集・分析・対策者の特定（2008-2009）

年月	対象	脆弱性の詳細	原因	対策
2008/10	組込アプリ	Webブラウザの乗っ取り	WebブラウザのオープンソースのWebKitの脆弱性を突いたバッファオーバフローでブラウザプロセスが乗っ取られる。	最新のライブラリを利用する。
2008/11	Android (root奪取)	telnet経由のroot侵入	ターミナルソフトをインストールして、ここからtelnetdを起動する。G1端末のIPアドレスにtelnet接続すると、認証なしでログイン。	ターミナルをユーザに提供しない。不要なサービスを削除して出荷する。
2008/11	端末H/W	アプリに対するキー入力をOSが実行(OSコマンドインジェクション)	シリアルポート接続されたデバイスのキー入力を受け取るinit.rcの設定が残っており、キーボード入力をOSが直接受け取っていた。	シリアルポート経由のアクセス設定を見直す。
2008/11	端末H/W	ログイン認証の無効化	menuキーを押し続けるとセーフモードで起動する。この場合、ログイン機能やスクリーンロック機能がパスされる。	セーフモードで起動した場合でも認証機能を設けておく。
2009/01	組込アプリ	URLの非表示によるフィッシングサイトへの誘導	Gmailブラウザにおいて、ハイパーリンクを閲覧できない問題と、FromとReply-toを閲覧できない問題がある。	GmailブラウザのURLやアドレス参照機能の設計に注意.
2009/02	組込アプリ	Webブラウザの乗っ取り	Webブラウザのサブシステム（PacketVideo）が利用するOpenCoreライブラリの脆弱性を突いたバッファオーバフロー攻撃を受ける。	OpenCoreライブラリのパッチを適用する。
2009/05	Android	公開アプリ認証の不具合	Android-SDKに、公開アプリ間のデータ参照や制御を自由に行えてしまうアプリ間認証の不具合があった。	uidの制御を修正するパッチをリリースした。
2009/05	Market	SDKにAndroid Market通信アプリのインストール	Android-SDKからでも、Android Marketと通信できるようにするSetupWizard.apk, gtalkservice.apk, Talk.apk, Vending.apkが公開。	Vending.apk(Market)アプリを公開させない。SDKと商用端末を見抜く機能が必要。
2009/08	Linux	ネイティブアプリのメモリダンプ	Linux用のメモリダンプツールを、ARM用にクロスコンパイルすることで、Android上のネイティブアプリのメモリダンプを取得できる。	秘匿性のある処理をメモリ上で行わない。ptraceなどの権限を最小化する。
2009/08	Linux (root奪取)	ファイルI/Oメモリ制御の不具合（CVE2009-2692）	CVE2009-2692のLinuxのメモリI/Oの初期化不具合を突いて、端末にrootでログインするマルウェア"asroot"が公開。	Linuxのパッチを適用する。
2009/09	公開アプリ	Web・FTP系アプリの公開	Web・FTPサーバ系の公開アプリをインストールすると、通信Portがオープンする。FTPはパスワード無しでログイン可。	—
2009/10	Market	MarketアプリのPCへのダウンロード（なりすまし端末）	Android Marketのフリーアプリのダウンロードに利用する4つのID（assetID, userID, device ID, authToken）を偽装できてしまう。	有料アプリのダウンロードについて、クライアント認証の仕組みを確認すべき。
2009/10	Android	SMSとDalvikの脆弱性でリモートから端末停止（CVE2009-2999）	SMSの脆弱性と、Dalvik APIの脆弱性がある。特殊なSMSパケットをAndroid端末に送りつけると、Dalvik上のサービスが停止する。	SMSとDalvik APIのパッチを適用する。（HT-03AはSMSの影響なし）
2009/10	端末H/W (root奪取)	カスタムROMのインストール（Recovery Utilityの改造）	CVE2009-2682でrootを奪取したHT-03A(v1.5)に対して、SDカード起動を許可する改造で、root付きROMをインストールできる。	Recovery Modeを排除すること。
2009/11	端末H/W	SIMロックの解除	HT-03A(1.5)の場合、端末コード（IEME）にリンク付けられたSIMロックを解除コード（PIN）の計算手法が解読されている。	SIMロックの解除コードを入力させるインタフェースを排除すればよい。
2009/11	公開アプリ	WiFiやBluetoothのホットスポットになり3Gへのテザリング	WiFiやBluetoothデバイスと3Gデバイスを接続してテザリングした。後位端末を見抜くことが出来ない。	iptablesでWiFi⇒3G通信を規制する。
2009/12	端末H/W (root奪取)	OSアップデートイメージの認証手法が漏洩してOSをダウングレード	純正HT-03A端末では、OSの配布元とバージョンを確認する検証コードが付与されている。この検証コードのアルゴリズムが漏洩。	OSをダウングレードさせないバージョンチェックを組み込む。

⚠ 警告　必ず、下記の警告事項をお読みになってからご使用ください。

禁止

落下させる、投げつけるなど強い衝撃を与えないでください。破裂・発熱・発火・漏液・故障の原因となります。

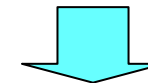
禁止

屋外で雷鳴が聞こえたときは使用しないでください。落雷・感電のおそれがあります。

分解禁止

IS03はソフトウェアも含め、お客様による分解・改造・変更・修理をしないでください。故障・発火・感電・傷害の原因となります。万一、改造などによりIS03またはソフトウェアなどに不具合が生じてもKDDI(株)・沖縄セルラー電話(株)では一切の責任を負いかねます。携帯電話の改造は電波法違反になります。

■ 端末改造抑止の呼びかけ

◆ ソフトを含む改造の禁止を呼びかけている。

公共の電波を発信する機器の適合基準を逸脱するソフト（OS）改造は違法です。

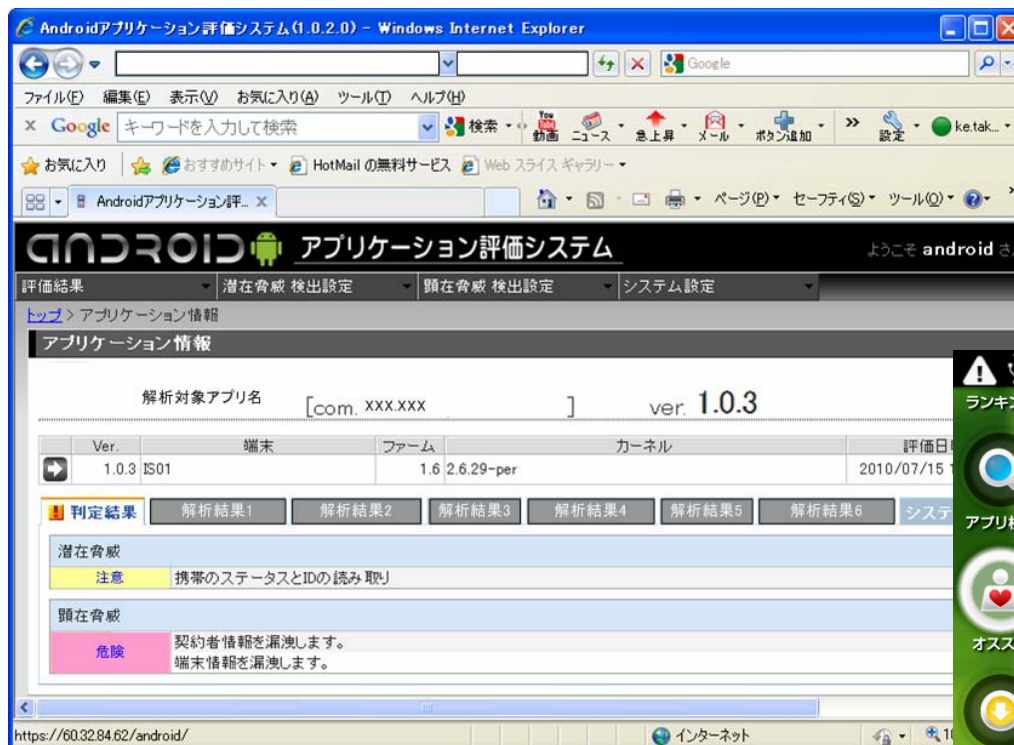
「Marketのセキュリティ」～セキュアアプリ検証～

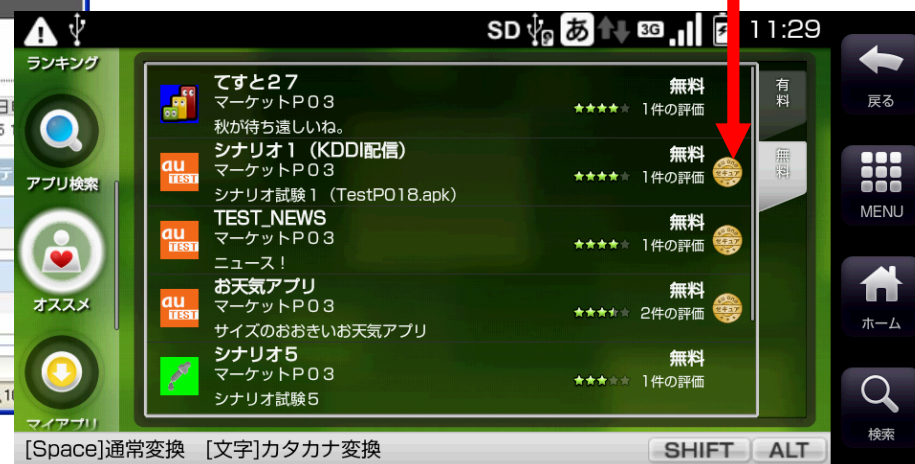
■ 世界初！事前評価のau one Market

★ Marketプレイスが安全になれば、脅威の多くを取り除ける。

◆ 潜在脅威（静的解析）：難解なAndroid™パーミッションの解読を、お客様に代わってKDDIが検証する。

◆ 顕在脅威（動的解析）：不審な挙動に注目して、お客様に代わってKDDIが検証する。

⇒ au one Marketセキュアアプリ検証を受けたアプリに、セキュアマークを付与している。

様々な独自技術でAndroid™向けアプリの安全性を評価

セキュアマーク

「アプリのセキュリティ」～開発者への啓発～

■ アプリ開発者への啓発活動

- ◆ 事前評価で確認するポイントを示すことで、安全なアプリ開発を促しています。
- ◆ 重要な情報を外部へ送信する場合には、アプリのストーリの中で、ユーザ承認を求めるようコメントしています。

チェックのポイント

1. 機能（パーミッション）
2. 本来利用できない機能の有無
3. 個人情報漏洩の有無
4. 外部への不正アクセス機能の有無

■ 安全性評価レポート（研究試作）

- ◆ パーミッションから推定される潜在脅威と挙動ログから判明した顕在脅威を解説。
- ◆ レポート生成の自動化を図り、アプリ開発者への啓発に利用する（予定？）。

Androidアプリケーション安全性評価レポート　2011/07/11

アプリケーション

	极品美女v1.0 [com.GoldDream.pg]
バージョン	1.0

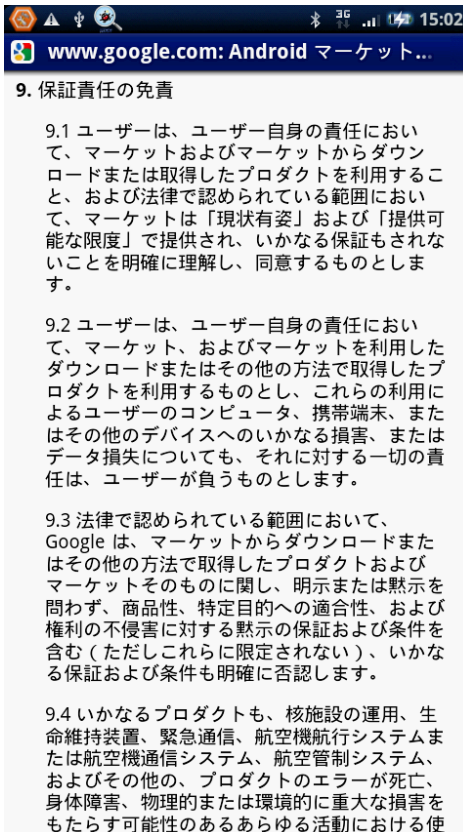
総合評価

危険	アプリを実行したときのログとアプリに潜在する能力を解析した結果、 危険な挙動と、悪用することで脅威となりうる機能が検出されました。

顕在脅威　－　アプリの動作ログや構成要素に注目し、危険な挙動や攻撃的な機能を抽出しています。

危険	情報漏洩	個人情報を漏洩するアプリです。
		端末情報を漏洩するアプリです。
		モバイル広告を利用するアプリです。
	攻撃	未検出
	不適切	管理者権限を必要とする不正なコマンドを実行するアプリです。

潜在脅威　－　アプリが利用する機能や情報に注目し、悪用された場合の脅威を評価しています。

危険	アプリケーションの削除
	アプリケーションを直接インストール
	電話番号発信
	SMSメッセージの送信
	おおよその位置情報（ネットワーク基地局）
	精細な位置情報（GPS）
	SMSの読み取り
	SMSの受信
	携帯のステータスとIDの読み取り
	発信の傍受
	起動時に自動的に開始

免責事項

「運用のセキュリティ」 ～お客様への説明～

■ 利用規約を通じた啓発活動

- ◆ 各Marketプレイスは、ユーザ責任でアプリのインストールについて注意喚起している。
- ◆ KDDIはさらに踏み込んで、端末の取扱説明書での注意書きや、ショップでの口頭説明＋承認プロセスを設けて、Marketプレイスの危険性に関する啓発活動に努めています。

Android Market™の免責

au one Marketの免責

IS01取扱説明書

免責事項について

◎地震・雷・風水害などの天災および当社の責任以外の火災、第三者による行為、その他の事故、お客様の故意または過失・誤用・その他異常な条件下での使用により生じた損害に関して、当社は一切責任を負いません。
◎本製品の使用または使用不能から生ずる附随的な損害（記録内容の変化・消失、事業利益の損失、事業の中断など）に関して、当社は一切責任を負いません。大切な電話番号などは控えておかれることをおすすめします。
◎本書と『取扱説明書詳細版』の記載内容を守らないことにより生じた損害に関して、当社は一切責任を負いません。
◎当社が関与しない接続機器、ソフトウェアとの組み合わせによる誤動作などから生じた損害に関して、当社は一切責任を負いません。
◎本製品の故障・修理・その他取り扱いによって、撮影した画像データやダウンロードされたデータなどが変化または消失することがありますが、これらのデータの修復により生じた損害・逸失利益に関して、当社は一切責任を負いません。
◎大切なデータはコンピュータのハードディスクなどに保存しておくことをおすすめします。万一、登録された情報内容が変化・消失してしまうことがあっても、故障や障がいの原因にかかわらず当社としては責任を負いかねますのであらかじめご了承ください。

Androidマーケットについて

◎アプリケーションのインストールは安全であることを確認のうえ、自己責任において実施してください。ウィルスへの感染や各種データの破壊などが発生する場合があります。
◎万一、お客様がインストールを行ったアプリケーションなどにより各種動作不良が生じた場合、当社では責任を負いかねます。
◎お客様がインストールを行ったアプリケーションなどにより、自己または第三者への不利益が生じた場合、当社では責任を負いかねます。

セキュリティ管理サービス ～OS層からの管理機構～

Android™携帯電話　管理サーバ

アクティベーション
(アプリ・ポリシ配信)

ポリシ設定
端末状態管理

インストールアプリ(アプリ層)

法人向けアプリA　B　・・・　アクティベーション（3LMアプリ）

アクティベート
アプリ・ポリシ

管理（3LMサーバ）

連携

セキュリティ管理付きAndroid OS(組込み層)

法人向け機能

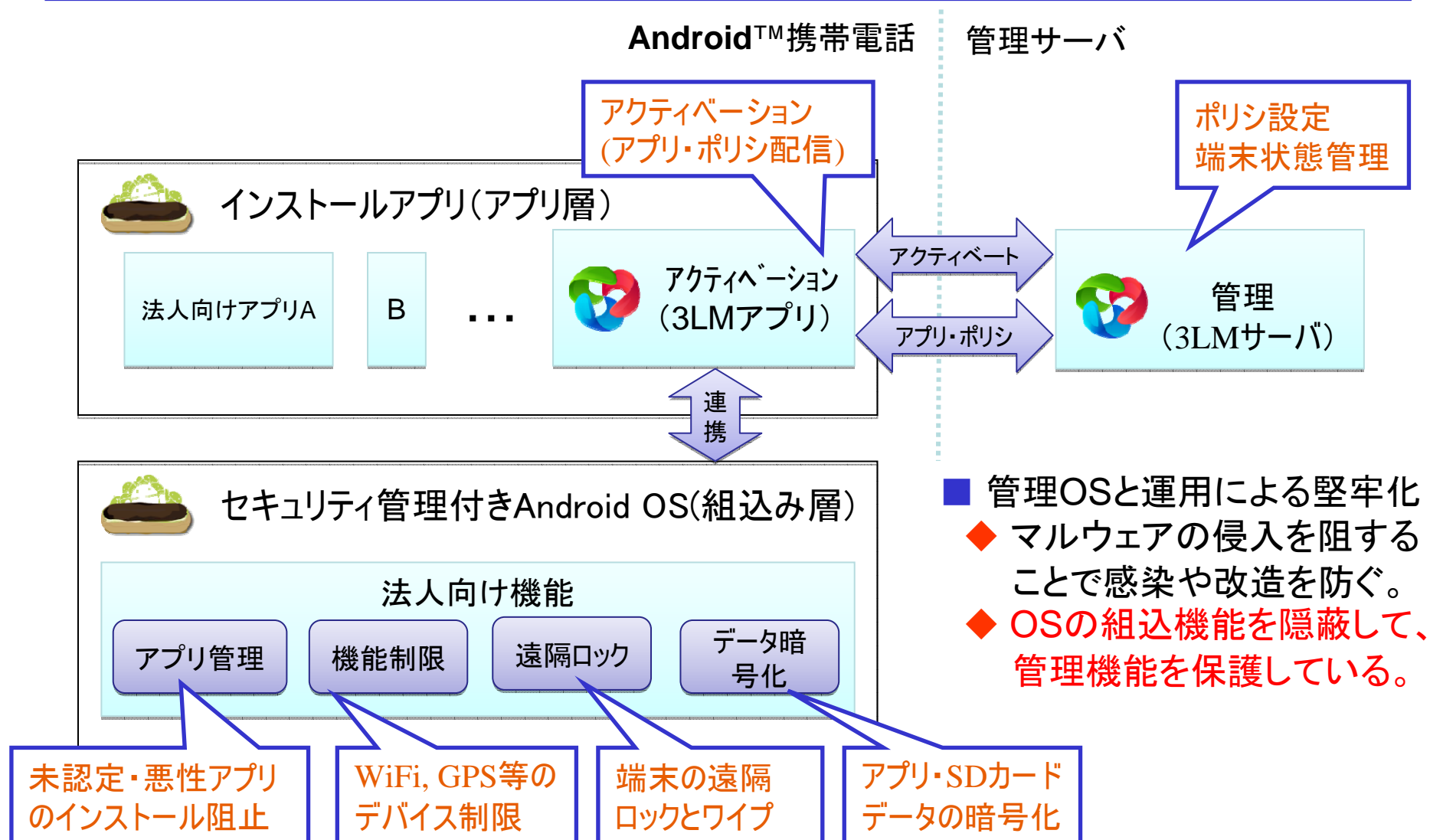
アプリ管理　機能制限　遠隔ロック　データ暗号化

未認定・悪性アプリのインストール阻止

WiFi, GPS等のデバイス制限

端末の遠隔ロックとワイプ

アプリ・SDカードデータの暗号化

- 管理OSと運用による堅牢化
  - マルウェアの侵入を阻することで感染や改造を防ぐ。
  - OSの組込機能を隠蔽して、管理機能を保護している。

MDM: Mobile Device Management

「端末の堅牢化」と「セキュリティ管理サービス」

■ 総合的な安全対策

◆ 端末の堅牢化とセキュリティ管理サービスの組み合わせで法人に適用できうる。

Player	要件	対策	詳細
端末メーカ	OS実装	ブートローダ保護	独自ディスク(ROM)への差替え阻止
		/system保護	/systemに対する改造阻止
	パッチリリース	パッチの適用	管理者権限奪取を阻止するパッチのリリース
MDMサービス	悪性Webサイト対策	URLフィルタ	URLのブラックリストを用いたフィルタリング
	マルウェア(悪性アプリ)対策	ブラックリスト(アンチマルウェア)	マルウェアのパターンファイルとの照合
		ホワイトリスト(認定アプリ)	アプリの安全性検証と認定 認定アプリのみインストールする制限機構
	社内網接続	VPN	暗号通信路＋認証による社内LAN接続
	ロック・ワイプ	リモートロック	ログインのためのパスワードのリモート制御
		リモートワイプ	工場出荷状態へ戻すリモート制御
	位置特定	GPS追跡	端末の位置情報をリモート監視
	機能制限	禁止機能の阻止	adbやWiFiなどのデバイス制限
	データの暗号化	データの暗号化	アプリデータを暗号化する機能
		SDカードの暗号化	SDカード全体に対する暗号化

MDM: Mobile Device Management

日本スマートフォンセキュリティフォーラム

■ 概要

- ◆ 通信キャリア、機器メーカ、システムインテグレータ、アプリケーション開発、サービス提供ベンダなどの 提供者だけではなく利用企業ならびに関連団体などが協調し、スマートフォンの安全な利活用を図り普及を促進するための任意団体です。

■ セキュリティへの活動内容

- ◆ 有益な情報の交換や提供を行う。
- ◆ 調査や研究を行う。
- ◆ スマートフォンセキュリティの普及、啓発を促進するための活動を行う。

■ 構成

- ◆ 技術部会
  ①ネットワークWG　②アプリWG
  ③デバイスWG　④脆弱性WG
- ◆ 利用部会
- ◆ 普及啓発部会

スマートフォンのセキュリティ

KDDI研究所
竹森 敬祐

新たな展開を目指して課題を整理しよう！

1: スマートフォンの概要
2: Android™フォンのセキュリティ
3: KDDIの取り組み
4: まとめ ～現状と今後の課題～

Android™は、Google Inc. の商標または登録商標です。

まとめ　～全体を通じて～

■ 世界標準の汎用OSの意味

◆ スマートフォンは、PCで培われた汎用OSが搭載されている。

× 従来の携帯電話の高機能版

○ PCに電話機能が付いたもの

◆ アプリインストールのリスクは、PCと同じく、ユーザに判断が委ねられている。

■ 逸脱行為の意味

◆ 端末／OS／アプリ／通信の各ベンダが適切に設定した端末を改造する行為は、本人のみならず他のユーザへも迷惑を掛ける可能性がある。

■ 法人利用でのMDM

◆ 遠隔から端末のセキュリティ等の状態を一元管理するMDMの導入が必要。

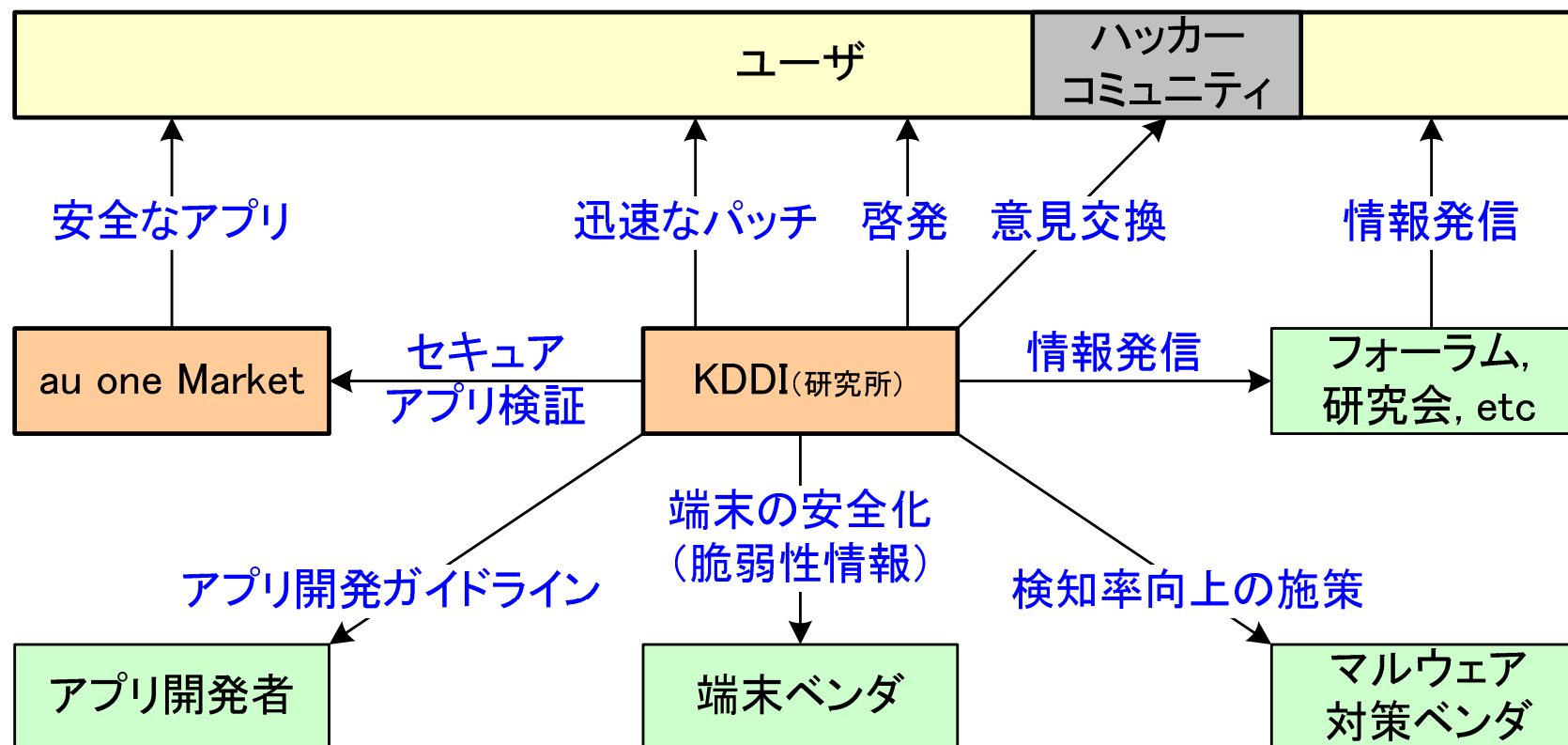
■ スマートフォンの安全管理の難しさ

◆ 端末中に、電気通信事業法に従う通信事業者のサービスと、比較的自由なインターネット事業者のサービスが同居している。

★ KDDIは、端末の堅牢化やau one Market等を通じて、通信キャリアの安全品質を提供する努力をさせて頂いております。

まとめ　～全体を通じて～

■ KDDIの取り組み
- ◆ 一般ユーザ: 安全なアプリ販売サイト“au one Market”における事前審査を実施。
- ◆ 法人ユーザ: 端末の堅牢化とデバイス管理のサービス化。
- ◆ 社会への貢献 ↓　注)「ハッカー」とは高度な知識を有する人材。攻撃者は「クラッカー」と呼ばれる。

ユーザ
ハッカーコミュニティ
安全なアプリ
迅速なパッチ
啓発
意見交換
情報発信
au one Market
セキュアアプリ検証
KDDI(研究所)
情報発信
フォーラム,研究会, etc
アプリ開発ガイドライン
端末の安全化(脆弱性情報)
検知率向上の施策
アプリ開発者
端末ベンダ
マルウェア対策ベンダ

スマートフォンセキュリティに関する通信事業者(KDDI)の取り組み

金融アプリの安全化　～今後の課題など～

■ 課題

- ◆ ソフトで管理・取得される認証子は、改竄される。
- ◆ 管理者権限が奪われた端末では、全てのファイルはReadされ、アプリの挙動はメモリダンプや通信ダンプでモニタされる。
- ◆ 複数人で共有する場合や紛失・盗難の場合を想定しなければならない。
- ◆ ブラウザのURL表示領域が小さく、接続先を参照し難い。

■ アプリの自己防衛

- ◆ 認証処理は、Javaコードから分離して、ネイティブコードで記述する。
- ◆ 認証子の暗号化、暗号鍵の安全な管理を施す。
- ◆ 管理者権限が奪われた場合には起動させない。

■ クライアント認証の安全化

- ◆ 暗証番号入力（記憶）などのユーザインタラクションを入れる。
- ◆ 通信キャリアに認証（SIM）を委託する。
- ◆ 生体認証デバイスを搭載する。

■ サーバ認証の安全化

- ◆ https通信、URLの全表示、など。

私からのメッセージ

■ ご利用の皆様へ

◆ 老若男女がPCを使いこなすように、スマートフォンも使いこなすことができます。
◆ その際、従来の携帯電話や組込み家電ではなく、PCと同じ危険にさらされます。
◆ ご自身のスマートフォンやその情報を守るために、最低限の対策をとって下さい。

対策1） アプリはOSベンダや通信キャリア等が提供する信頼できるマーケットから入手してください。
対策2） アプリの導入時に注意書きが表示される場合には、これを良く読み、リスクを判断してください。
対策3） 端末を更新するソフト（パッチ）が提供された場合には、迅速に適用ください。
・・・

■ 通信キャリアやJSSECによる支援

◆ スマートフォンの開発は、世界市場が先行しています。従って、契約・承認の手続きが入っていたり、日本人には馴染みが薄く、理解し難いものもあります。
◆ 通信キャリア、端末メーカ、セキュリティ対策ベンダ、アプリケーション開発者、コンテンツパブリッシャーが、様々な支援サービスを提供しています。
◆ 我々は、個人や企業単位で解決できない、スマートフォンを安全に使って頂くための様々な情報提供ならびに施策を進めてまいります。